

Appendix D

AIS Certification and Accreditation

A. CERTIFICATION

The ISSR, working jointly with the Customer, is responsible for coordinating and supporting the certification process. The ISSR is responsible for certifying, or coordinating the certification of, the AIS or network. Certification, which is a prerequisite for accreditation, is accomplished as follows:

1. **Identify** operational requirements, define the *Mode of Operation*, and identify applicable security requirements, in accordance with this document and applicable documents referenced herein.
2. Conduct a *Risk Management Review* to identify risks and needed countermeasures and specify additional security requirements (countermeasures) based on the **review**.
3. Prepare an **AISSP**. Refine the plan throughout the certification process.
4. Conduct a test and inspection to establish the extent to which the AIS performs the **security** functions needed to support the mode of operation and security policy for the system as outlined in the AISSP. The Customer will require a written certification report.
5. Operating in the **compartmented** or multilevel mode requires the development of an *AIS Technical Evaluation Plan*. After Customer concurrence, accomplish testing as described herein. AIS security testing provides assurance to the Customer that the subject **AIS(s)** or network(s) meets the security requirements for operating in the compartmented or multilevel mode. Such testing is a prerequisite for Customer accreditation.
 - a. Coordination Scheduling and Testing. The security test may be jointly conducted by the Provider and the Customer.
 - b. Testing Prerequisite. The Provider-developed *AIS Technical Evaluation Test Plan* will be coordinated **and/or** approved by the customer.

B. ACCREDITATION

Accreditation is the Customer's authorization and approval for an AIS or network to process sensitive data in an operational environment. The Customer bases the accreditation on the results of the certification process. Following certification, the Customer reviews the risk assessment, employed safeguards, **vulnerabilities**, and statement of level of risk and makes the accreditation decision to accept risk and grant approval to operate; grant *interim approval to operate (IATO)* and fix deficiencies; or to shut-down, fix deficiencies, and recertify.